ABSTRACT OF THE INVENTION

A computer system (20) with a security domain (22), at least one client business domain (26), and a plurality of client terminals (34) utilizes a hidden link dynamic key manager (24, 84) and a database structure including encrypted data entities (30C, 30D) and a security identification attribute (32) for storage of encrypted data. A method for encryption, storage, decryption, and retrieval of encrypted data operates on the computer system (20), which also includes an information database (62) and a key database (44). The key database (44) is isolated from the information database (62). The security domain (22) includes a system key manager (84) operable to generate system keys with system key common names and an encryption key manager (24) operable to generate encryption keys having encryption key identifications. The key managers (24, 84) operate on a key server (40), which is mirrored by a secondary key server (42). A general security manager (82) also operates on the key server (40) to control access to the security domain (22). The security information attribute (32) is stored with a persistent data entity (30A) that is associated with the other data entities (30C, 30D) by a database schema. The security information attribute (32) includes the encryption key identification (112) for the encryption key used to encrypt the data entities (30C, 30D). The encryption key identification is encrypted by the system key, and the system key common name hash value (114) is also stored in the security information attribute (32). The information data entities (30) are stored on the information database (62), but the encryption key identification (153), encryption key (154), system key common name hash value (156, 157), and system key common name (158) are stored in the key database (44) inside the security domain (22). The system key itself is stored on a Smart Card reader (56) inside the security domain.